

# Learning from Failures: Archiving and Designing with Failure and Risk

Michael Van Wie, Matt Bohm, Francesca Barrientos, Irem Tumer, Robert Stone  
**Keywords** – *failure analysis, risk assessment, failure taxonomy, reliability based design*

## OBJECTIVES

The main goal of this work is to illustrate how past failures can be used for understanding failures, risks, and the processes used to elicit failures and risks during design. Through an examination of past failure data as well as observational studies of designers, this work shows how failures and risks can be archived and subsequently used during conceptual design.

## METHODS

This research adopts two approaches in order to address i) past instances of failures and ii) the elicitation and treatment of failures and risks during design. The task begins with a brief study of the theory supporting the representation issues associated with properly describing failure and risk information. Concepts such as failure taxonomy and the metrics of likelihood, impact, and uncertainty are used to provide a consistent context for describing failure information. Given these basic fundamentals of failure representation, the research examines current tools that are used from a variety of organizations including the NTSB, DOT, NASA, and a product repository at UMR as they relate to archived failure data. A study of these tools serves two purposes. First, it illustrates a variety of challenges related to storing and utilizing failure data to achieve meaningful results. Several uses of failure data are evidenced through observations of these tools. The use of such failure data during design leads to the second overall approach in this research: examining how designers use failure data during conceptual design. Direct observations of a design team at JPL during mission designs are performed in order to determine how risks are addressed at the conceptual stage of design.

## RESULTS

The results of this work show that certain types of information are common among various organizations that archive design failure data. Based on consideration of the failure data in the various archival tools examined in this work, a set of design activities and interactions with these tools are hypothesized. These design actions establish a description of the tasks and modes in which designers can currently use such archived failure information. This provides evidence for understanding what capabilities are important for future repository development efforts in terms of how failure data is accessed and used. Based on the observations of a JPL design team (Team X), a description of how designers account for failures and risk during a fast paced conceptual design environment is established. This description includes both procedural

information as well as details and examples of the language and format in which failure and risk data is used. Due to the nature of conceptual design, much of the failure and risk information is treated verbally during the observed sessions. A great amount of variation is exhibited in the verbal descriptions and references to failures where these variations propagate to variations in how failures and risks are formally documented and reported. Our observations show that these variations appear at both a syntax level and a semantic level. One particular highlight of this description is a set of mappings that relate high level conceptual design information with specific failure and risk data. Embedded in this set of relations is an association between function and failure data that is based on recent work toward the development of a Function-Failure Design tool.

## **CONCLUSIONS**

The main conclusions show how data from past instances of failures can be used in an archived format for supporting several design activities. By adopting a consistent taxonomy of failures and a sensible data framework for collections of failure data, this work demonstrates how archived failure data can be stored, accessed, and used effectively. Beyond the use of these tools, the second thrust of this work shows that during conceptual design, failures are addressed at multiple levels of abstraction depending on the problem being solved. The variations found in the references to failure and risk information during conceptual design suggest that despite an existing failure taxonomy, designers could still benefit from advanced failure and risk tools for conceptual design activities. An ongoing challenge is to define a workable interface that increases designer awareness of potential failures while minimizing the workload and training curve associated with any new design methods or tools.

## **REFERENCES**

Barney, R. and Bennet, R., "Risk Management for the NASA/JPL Genesis Project: A Case Study," *10th Annual International Symposium of the International Council on Systems Engineering*, (INCOSE-2000) Minneapolis, Minnesota, June 16-20, 2000.

Bohm, M. and Stone, R., "Product Design Support: Exploring a Design Repository System," *ASME International Mechanical Engineering Congress IMCE 2004-61746*.

Feather, M. and Cornford, S., "Quantitative Risk-Based Requirements Reasoning," *Requirements Engineering Journal (forthcoming special issue)*.

Meshkat, L., Cornford, S., Moran, T., "Risk Based Decision Tool for Space Exploration Missions," *American Institute of Aeronautics and Astronautics Space Conference and Exhibition, AIAA 2003-6377*.

Stone, R., Tumer, I., Van Wie, M., "The Function-Failure Design Method," *Journal of Mechanical Design* [in press].